

## **REMARKS**

Claims 1-27 are pending. Claims 13 and 14 are allowed. Claims 1 and 15 have been amended. In view of the following, all pending claims are in condition for allowance. If, after considering this response, the Examiner does not agree that all of the claims are allowable, he is requested to schedule a teleconference with the Applicants' attorney to further the prosecution of the application.

### **Rejection of claims 1-12 under 35 U.S.C. §112, second paragraph**

Claim 1 has been amended to overcome this rejection.

### **Rejection of claim 20 under 35 U.S.C. §112, first paragraph**

Claim 20 recites generating the first pseudo-random value from a previous chaos-based pseudo-random value. Such a limitation is supported, for example, by paragraphs 54 and 82 of the present application. The method of generating a chaos-based pseudo-random value "could be easily repeated" so that the chaos-based pseudo-random value of a generator can be used by other "generators of sequences of pseudo-random numbers" (paragraph 54).

### **Rejection of claims 1-12 and 15-25 under 35 U.S.C. §101**

Claims 1 and 15 have been amended to overcome this rejection.

### **Rejection of claims 1-3, 5-7 and 15-27 under 35 U.S.C. §102(e) as being anticipated by Butler (US 6,678,707)**

#### **Claim 1**

Claim 1 recites generating numbers of a pseudo-random sequence and calculating numbers of a chaos-based pseudo-random sequence by applying a function to corresponding integer numbers of the pseudo-random sequence, where the inverse of the function has a plurality of branches.

For example, referring, e.g., to paragraphs 52-70 of the present application, a method includes generating numbers of a pseudo-random sequence  $x_n$  and calculating

numbers of a chaos-based pseudo-random sequence  $X_n$  by applying a function  $H(x)$  to corresponding integer numbers of the pseudo-random sequence  $x_n$ , where the inverse of the function  $H(x)$  has a plurality of branches.

Butler, on the other hand, does not disclose generating numbers of a pseudo-random sequence and calculating numbers of a chaos-based pseudo-random sequence by applying a function to corresponding integer numbers of the pseudo-random sequence, where the inverse of the function has a plurality of branches. Instead, Butler addresses the problem of generating truly random numbers (col. 4, lines 35-40). As a result, Butler cannot be used in cryptographic codes in which the receiver of the data needs to reconstruct the random number sequence to decrypt the data because Butler generates a sequence of truly random numbers that is unpredictable even if the seed is known. Specifically, Butler discloses a means 800 that carries out a post-processing algorithm for eliminating all possible correlations/dependencies between successive random numbers generated by a MISR 402-412 (FIG. 8; col. 8, lines 5-27). The means 800 does not generate a sequence of chaos-based pseudo-random numbers by evolving from a given pseudo-random number used as a seed, but instead calculates only one truly random number as a function of the current random number (and possibly as a function of previous random numbers) generated by the MISR 402-412 using a hash function or another function (col. 8, lines 16-27). Therefore, Butler does not satisfy the limitations of claim 1.

#### **Claims 15 and 26-27**

Claims 15 and 26-27 are patentable for reasons similar to those recited above in support of the patentability of claim 1.

#### **Claims 2-3, 5-7 and 16-25**

Claims 2-3, 5-7 and 16-25 are patentable by virtue of their respective dependencies from claims 1 and 15.

## CONCLUSION

In light of the foregoing, claims 1-27 are in condition for allowance, which is respectfully requested.


If the Examiner determines that additional fees are necessary, he is authorized to charge them to deposit account number 07-1897.

If, after considering this response, the Examiner does not agree that all of the claims are allowable, then it is respectfully requested that the Examiner schedule a phone interview with the Applicants' attorney at (425) 455-5575.

Dated this 25<sup>th</sup> day of June, 2007.

Respectfully submitted,

GRAYBEAL JACKSON HALEY LLP



---

J. Mark Han  
Attorney for Applicant  
Registration No. 57,898  
155 - 108th Avenue N.E., Suite 350  
Bellevue, WA 98004-5973  
Phone: (425) 455-5575  
Fax: (425) 455-1046